AMENDMENTS TO THE CLAIMS

1. **(Currently Amended)** A content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the content distribution server comprising:

a key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

an encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

a content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using the at least one node encryption key in the selected node encryption key group;

a content receiving unit operable to receive a content via the network;

an encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key; and

a transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses,

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0^{th} level through an nth level, n being 1 or a larger natural number; and

selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes, and

said encryption key group selection unit ~~selects at least one terminal node from among the terminal nodes, and~~ selects the selected node encryption key group so that the selected node encryption key group includes [[a]] at least one node encryption key that is set for ~~the selected~~ a terminal node and [[a]] at least one node encryption key that is set for a node other than the ~~selected~~ terminal [[node]] nodes by randomly selecting a node encryption key that is set for a

terminal node among the terminal nodes and then further selecting a node encryption key assigned to a content output apparatus to which the selected node encryption key is not assigned.

2. **(Canceled)**

3. **(Previously Presented)** The content distribution server according to Claim 1, wherein the tree structure in the key assignment method is an N-ary tree, N being 2 or a larger natural number.

4. **(Previously Presented)** The content distribution server according to Claim 1, further comprising

a content key generation unit operable to newly generate at least one pair of a content encryption key and a corresponding content decryption key which is different from at least one pair of a content encryption key which is previously used for encrypting a content and a corresponding content decryption key, in the case where said content receiving unit receives a new content.

5. **(Currently Amended)** The content distribution server according to Claim 1, wherein said encryption key group selection unit newly selects ~~a selected node encryption key group including~~ a node encryption key that is set for another terminal node than a previously selected terminal node, in the case of receiving a new content via said content receiving unit[[.]] when selecting the node encryption key that is set for the at least one terminal node among the terminal nodes.

6. **(Previously Presented)** The content distribution server according to Claim 1, further comprising

a key selection information storage unit operable to hold a plurality of key selection information which are used for selecting the node encryption key included in the node encryption key group,

wherein said encryption key group selection unit selects the selected node encryption key group based on the key selection information.

7. **(Previously Presented)** The content distribution server according to Claim 6,

wherein said key selection information storage unit further holds a plurality of key selection identifiers that identify the key selection information, the key selection identifiers and the key selection information being associated with each other,

said encryption key group selection unit selects the selected node encryption key group based on the key selection information, and

said transmission unit distributes, to the content output apparatuses, the encrypted content, the encrypted content decryption key group and the key selection identifiers associated with the key selection information.

8. **(Previously Presented)** The content distribution server according to Claim 6,

wherein said encryption key group selection unit selects, on a random basis, one of the key selection information from among the plurality of key selection information held in said key selection information storage unit, and selects the selected node encryption key group based on the selected key selection information.

9. **(Previously Presented)** The content distribution server according to Claim 6,

wherein said encryption key group selection unit selects, at regular intervals, one of the key selection information from among the plurality of key selection information held in said key selection information storage unit, and selects the selected node encryption key group based on the selected key selection information.

10. **(Previously Presented)** The content distribution server according to Claim 1, further comprising

a storage unit operable to store the node encryption key group received via the network into said key information storage unit.

11-26. **(Canceled)**

27. **(Currently Amended)** A content distribution system comprising content output apparatuses and a content distribution server, each of the content output apparatuses decrypting an encrypted content using a content decryption key and outputting the decrypted content, and a content distribution server creating an encrypted content by encrypting a content, and distributing the encrypted content to each content output apparatus via a network,

wherein said content output apparatus includes:

a first receiving unit operable to receive the encrypted content and an encrypted content decryption key group which are distributed from the content distribution server;

a second receiving unit operable to receive, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method;

a node key storage unit operable to hold the node decryption key group;

a decryption key obtaining unit operable to obtain the content decryption key based on at least one node decryption key group and at least one encrypted content decryption key group; and

a first decryption unit operable to decrypt the encrypted content using the content decryption key, and

said content distribution server includes:

a key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

an encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

a content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group;

a content receiving unit operable to receive a content via the network;

an encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key; and

a transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses,

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0^{th} level through an nth level, n being 1 or a larger natural number; and

selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes, and

said encryption key group selection unit ~~selects at least one terminal node from among the terminal nodes, and~~ selects the selected node encryption key group so that the selected node encryption key group includes [[a]]at least one node encryption key that is set for ~~the selected~~a terminal node and [[a]]at least one node encryption key that is set for a node other than the ~~selected~~ terminal [[node]]nodes by randomly selecting a node encryption key that is set for a terminal node among terminal nodes and then further selecting a node encryption key assigned to a content output apparatus to which the selected node encryption key is not assigned.

28. (**Original**) The content distribution system according to Claim 27, further comprising a key issuing center that is connected, via a network, with the content distribution server and the content output apparatuses, and issues a key for obtaining a content decryption key to each of the content output apparatuses,

wherein the key issuing center includes:

a node key generation unit operable to generate, based on a predetermined key assignment method, a node encryption key group that is a set of node encryption keys and a node decryption key group that is a set of node decryption keys, each of the node encryption keys and node decryption keys being assigned to each content output apparatus;

a first transmission unit operable to transmit the node encryption key group to the content distribution server;

a node decryption key group selection unit operable to select at least one of the node decryption keys, and generate the node decryption key group to be distributed to each content output apparatus; and

a second transmission unit operable to distribute the node decryption key group to the content output apparatus.

29. (**Currently Amended**) A computer-readable recording medium on which a program is recorded, the program being used for a content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the program comprising:

holding a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

selecting, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

generating an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group;

receiving a content via the network;

encrypting the content using a content encryption key which is previously given as a pair with the content decryption key; and

distributing the encrypted content and the encrypted content decryption key group to the content output apparatuses,

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0^{th} level through an nth level, n being 1 or a larger natural number; and

selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes, and

said encryption key group selection unit ~~selects at least one terminal node from among the terminal nodes, and~~ selects the selected node encryption key group so that said selected node encryption key group includes [[a]]at least one node encryption key that is set for ~~the selected~~a terminal node and [[a]]at least one node encryption key that is set for the selected terminal node and node encryption key that is set for a node other than the ~~selected~~ terminal [[node]] [[node]]nodes by randomly selecting a node encryption key that is set for a terminal node among terminal nodes and then further selecting a node encryption key assigned to a content output

apparatus to which the selected node encryption key is not assigned.

30-33. **(Canceled)**

34. **(Currently Amended)** A content distribution method to be used for a content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the method comprising:

holding a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

selecting, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

generating an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group;

receiving a content via the network;

encrypting the content using a content encryption key which is previously given as a pair with the content decryption key; and

distributing the encrypted content and the encrypted content decryption key group to the content output apparatuses,

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0th level through an nth level, n being 1 or a larger natural number; and

selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes, and

said encryption key group selection unit ~~selects at least one terminal node from among the terminal nodes, and~~ selects the selected node encryption key group so that said selected node encryption key group includes [[a]]at least one node encryption key that is set for ~~the selected~~a

terminal node and [[a]]at least one node encryption key that is set for a node other than the ~~selected~~ terminal [[node]] nodes by randomly selecting a node encryption key that is set for a terminal node among the terminal nodes and then further selecting a node encryption key assigned to a content output apparatus to which the selected node encryption key is not assigned.

35-39. **(Canceled)**